AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for computer security to control access to data held on a computer system as requestable datasets, said method comprising the steps of:

allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each user group corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

providing for each dataset a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

giving access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership ~~in~~of that user group and members of that user group being associated with a common ~~data~~dataset access category ~~for~~which enables access to that dataset.

2. (currently amended) A method according to Claim 1, wherein the user groups and data access categories have hierarchical levels in which a higher dataset access category incorporates

a or, as the case may be, each lower dataset access category, and the method includes allowing access to datasets by members of user groups associated with dataset access category levels equal to and higher than those to which such datasets correspond.

3. (previously presented) A method according to Claim 1, wherein each user is associated with a computer-based identifying certificate means and the method includes the step determining a user's identity from the identifying certificate means.

4. (previously presented) A method according to Claim 3, wherein the computer-based identifying certificate means is an X.509 certificate.

5. (previously presented) A method according to Claim 1, wherein the datasets are web pages and the method includes the step of gaining access to the computer network via the Internet or the World-Wide-Web.

6. (original) A method according to Claim 1, wherein the datasets are web pages and the step of associating each dataset with a dataset access category comprises inserting meta tags in html web page code.

7. (previously presented) A method according to Claim 1, further including the step of performing a challenge-response exchange regarding user identification before the step of giving access to a dataset.

8. (currently amended) A method according to Claim 1 in which a user group member employs a user computer system to gain access to datasets to which access is controlled by an access control computer system having a public key for verifying signed data, wherein each user computer system incorporates a private key for signing data and user group identifying means, and the dataset access step includes:

using the private key to sign test data provided by the access control computer system and forwarding the signed data and user group identity information provided by the identifying means to the access control computer system; and

using the access control computer system to;

verify the user group identity information,

verify the user by using the public key to verify the signed data, and

determine user group and associated dataset access category from the user group identity information.

9. (original) A method according to Claim 8, wherein the test data is random data.

10. (original) A method according to Claim 1, further including the step of providing database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

11. (original) A method according to Claim 1, wherein data is maintained on at least one database computer system, dataset access is given by access control software operated on a separate access control computer system, and a user gains access to data by means of

access request software running on a user computer system separate from the database and access control computer systems.

12. (original) A method according to Claim 11, wherein the access control software is configured with a firewall protecting a database computer system.

13. (previously presented) A method according to Claim 11, wherein data is maintained on a plurality of database computer systems and, in response to a data request, access control software determines whether or not corresponding data access is appropriate after relaying the request to a database computer system having such data.

14. (original) A method according to Claim 1, wherein data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the step of giving dataset access involves comparing user group and dataset numerical values to determine whether or not access is to be granted or denied.

15. (original) A method according to Claim 14, wherein the data access categories have different sections each with a section numerical value and the step of comparing numerical values comprises comparing section numerical values of corresponding sections of user group and dataset numerical values.

16. (original) A method according to Claim 14, wherein access to a dataset is provided only if all section comparisons are satisfied.

17. (original) A method according to Claim 1, wherein the step of giving access to a dataset includes unencrypted transfer of data from datasets to which access is granted.

18. (previously presented) A method according to Claim 16 wherein a user has a user computer system, and wherein the method includes the step of running checking/blocking software on the user computer system to screen incoming data for encryption to block unwanted data content.

19. (currently amended) A computer program product comprising a computer readable medium containing computer readable instructions for controlling operation of a computer system and providing control of access to data held on a computer system as requestable datasets each having an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by computer system users, wherein the computer readable instructions provide a means for controlling the computer system to:

(a) receive data requests from human users of a computer system allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each user group being associated with a respective one of said data access categories such that all members of a user group having multiple members are associated with a dataset access category which is common to members of that user group;

(b) control access to datasets each of which is associated with a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

(c) give access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category ~~for~~which enables access to that dataset.

20. (currently amended) A computer program product according to Claim 19, wherein the user groups and data access categories have hierarchical levels in which a higher dataset access category incorporates a or, as the case may be, each lower dataset access category, and the computer readable instructions allow access to datasets by members of user groups associated with dataset access category levels equal to and higher than those to which such datasets correspond.

21. (previously presented) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for determining a user's identity from computer-based identifying certificate means.

22. (previously presented) A computer program product according to Claim 21, wherein the computer-based identifying certificate means is an X.509 certificate.

23. (original) A computer program product according to Claim 19, wherein the datasets are web pages and the computer readable instructions enable access to the web pages via the Internet or the World-Wide-Web.

24. (original) A computer program product according to Claim 19, wherein the datasets are web pages and the computer readable instructions provide a means for identifying dataset access categories in web pages from meta tags in html web page code.

25. (previously presented) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for challenging incoming data requests regarding user identification before giving access to a dataset.

26. (currently amended) A computer program product according to Claim 19 for interacting with a user computer system incorporating a private key for signing data and user group identifying means, wherein the computer readable instructions provide a means for controlling the computer system to:

(a) send test data to the user computer system for signature with the private key and return with user group identity information provided by the identifying means,

(b) verify the user group identity information,

(c) verify the user by using the public key to verify the signed data, and

(d) determine user group and associated dataset access category from the user group identity information.

27. (original) A computer program product according to Claim 26, wherein the test data is random data.

28. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

29. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide a firewall for a database computer system.

30. (original) A computer program product according to Claim 19, wherein data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the computer readable instructions provide a means for granting or denying dataset access on the basis of comparison of user group and dataset numerical values.

31. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for transferring dataset material to appropriate recipients unencrypted.

32. (currently amended) A network access controller for controlling access to data held on a computer system as requestable datasets, wherein the controller:

(a) receives data requests from human users of a computer system allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each user group corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

(b) controls access to datasets each of which is associated with a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

(c) gives access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category ~~for~~which enables access to that dataset.

33. (original) A controller according to Claim 32, wherein the controller compares numerical values associated with data access categories of datasets and user groups in order to determine whether or not to grant access to data.

34. (original) A controller according to Claim 32, wherein said controller provides database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

35. (currently amended) A computer network for database access by human users having identifying certificates and allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identifying certificate information common to such members, wherein said network treats each user group as corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group, and includes:

(a) an access controller controlling access to a database comprising a plurality of datasets each having an associated dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by users;

(b) means for verifying human users;

(c) a database of datasets each of which is associated with a dataset access category selected from said plurality of such categories; and

(d) computer software arranged to give access to a dataset to a member of a user group with multiple members in response to such member providing identifying certificate information as evidence of membership of that user group and members of that user group being associated with a common dataset access category ~~for~~which enables access to that dataset.

36. (original) A network according to Claim 35, wherein the database comprises web pages in which dataset access categories are implemented by insertion of meta tags in web page html code.

37. (original) A network according to Claim 35, wherein said network is an Internet or World-Wide Web network.

38. (currently amended) A method for controlling user access to data held on a computer system as requestable datasets, the method including:

labelling the datasets with dataset access labels defining a hierarchy of data access levels eachselected from a plurality of data access levels and associated with a criterion for access to thata dataset by computer system users,

allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership inof a user group having multiple members is authentically evidenced by provision of user group identity information common to such members,

labelling user groups with data access levels selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group; and

giving access to a requested dataset to a requesting member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested dataset.

39. (previously presented) A method according to claim 38 wherein the datasets are web pages with dataset access labels which are meta tags, and a proxy server is used to:

receive requests for web pages from members of user groups,

check user group data access levels against a prearranged access control list, and

deny members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

40. (currently amended) A method for controlling user access to data held on a computer system as requestable web pages, the method including:

(a) labelling the web pages with meta tags defining a hierarchy of data access levels for an access control list providing a plurality of data access levels each associated with a criterion for access to a dataset by computer system users,

(b) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) labelling user groups with respective data access levels associated with member groupings and selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group,

(d) using a proxy server to:

receive a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

send data for signature to the client computer system and obtain the requesting member's certificate,

receive data from the client computer system,

verify that the received data is:

(1) signed with the requesting member's key,

(2) a signed equivalent of the data sent to the requesting member for signature, and

(3) signed with a key from a certificate which is not time expired or invalid,

if the received data is verified as aforesaid, check the data access level of the requesting member's user group against the access control list, and

give access to a requested web page to the requesting member if said requesting member is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested web page.

41. (previously presented) A network access control system for controlling access to data held on a computer system as requestable datasets, the control system being arranged to:

(a) label the datasets with dataset access labels defining a hierarchy of data access levels,

(b) communicate with human computer system users allocated between a plurality of human user groups,

(c) label said user groups with data access levels selected from a plurality of such levels; and

(d) give access to a requested dataset to a requesting human member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested dataset.

42. (previously presented) A network access control system according to claim 41 wherein the datasets are web pages with dataset access labels which are meta tags and the control system has a proxy server for:

(e) receiving requests for web pages from members of user groups,

(f) checking user group data access levels against a prearranged access control list, and

(g) denying members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

43. (currently amended) A network access control system for controlling user access to data held on a computer system as requestable web pages, the control system being arranged to:

(a) label the web pages with meta tags defining a hierarchy of data access levels for an access control list providing a plurality of data access levels each associated with a criterion for access to a dataset by computer system users,

(b) allocate human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group

identity information common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) label user groups with respective data access levels associated with member groupings and selected from said plurality of member groupings such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group,

and the control system has a proxy server for:

(i) receiving a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

(ii) sending data for signature to the client computer system and obtain the requesting member's certificate,

(iii) receiving data from the client computer system,

(iv) verifying that the received data is:

signed with the requesting member's key,

a signed equivalent of the data sent to the requesting member for signature, and

signed with a key from a certificate which is not time expired or invalid,

(v) if the received data is verified as aforesaid, checking the data access level of the requesting member's user group against the access control list, and

(vi) giving access to a requested web page to the requesting member if it is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested web page.

44. (currently amended) A method for computer security to control access to data held on a computer system as requestable datasets, the method including:

(a) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members;

(b) providing for each dataset an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group and membership of a user group having multiple members is authentically evidenced by provision of like user group information by each of such multiple members; and

(d) providing access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access to that dataset.

45. (currently amended) A method for computer security to control access to data held on a computer system as requestable datasets characterised in that the method includes:

(a) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership ~~in~~of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members;

(b) providing for each dataset an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

(d) providing a respective computer-based identifying certificate means for each user containing said user group identity information; and

(e) providing access to a dataset to a member of a user group with multiple members in response to such member providing identifying certificate means and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access to that dataset.